CLAIMS

What is claimed is:

1. A method of automatically establishing differentiated services quality of service treatment for a return packet flow that is associated with an originating packet flow in a network, the method comprising the computer-implemented steps of:

receiving the originating packet flow;

determining that one or more packets in the originating packet flow are marked with a DSCP value that matches a policy rule that requires setting a specified DSCP value in the return packet flow;

creating and storing information identifying the originating packet flow and a second DSCP value for marking the return packet flow;

receiving the return packet flow and determining that it is associated with the originating packet flow;

marking packets of the return packet flow with the second DSCP value.

2. A method as recited in Claim 1, wherein the information identifying the originating packet flow and the second DSCP value are created and stored in a flow table of a network switch that is acting as a policy enforcement point.

3. A method as recited in Claim 1, wherein the information identifying the originating packet flow and the second DSCP value are created and stored in a network-based application recognition table of a network switch that is acting as a policy enforcement point.

4. A method as recited in Claim 1, further comprising the steps of:

identifying an end of the originating packet flow;

removing the stored information that identifies the originating packet flow and a second DSCP value for marking the return packet flow.

5. A method as recited in Claim 1, wherein the steps are carried out at a switch device that is logically located at an edge point of a network.

6. A method as recited in Claim 1, wherein creating and storing information comprises creating and storing a static policy at a policy server, wherein the static policy specifies applying the second DSCP value to the return packet flow.

7. A computer-readable medium carrying one or more sequences of instructions for automatically establishing differentiated services quality of service treatment for a return packet flow that is associated with an originating packet flow in a network, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:
receiving the originating packet flow;
determining that one or more packets in the originating packet flow are marked with a DSCP value that matches a policy rule that requires setting a specified DSCP value in the return packet flow;
creating and storing information identifying the originating packet flow and a second DSCP value for marking the return packet flow;
receiving the return packet flow and determining that it is associated with the originating packet flow;
marking packets of the return packet flow with the second DSCP value.

8. A computer-readable medium as recited in Claim 7, wherein the information identifying the originating packet flow and the second DSCP value are created and stored in a flow table of a network switch that is acting as a policy enforcement point.

9. A computer-readable medium as recited in Claim 7, wherein the information identifying the originating packet flow and the second DSCP value are created and stored in a network-based application recognition table of a network switch that is acting as a policy enforcement point.

10. A computer-readable medium as recited in Claim 7, wherein the steps are carried out at a switch device that is logically located at an edge point of a network.

11. A computer-readable medium as recited in Claim 7, wherein creating and storing information comprises creating and storing a static policy at a policy server, wherein the static policy specifies applying the second DSCP value to the return packet flow.

12. A computer-readable medium as recited in Claim 7, further comprising instructions for carrying out the steps of:
identifying an end of the originating packet flow;
removing the stored information that identifies the originating packet flow and a second DSCP value for marking the return packet flow.

13. An apparatus that can automatically establishing differentiated services quality of service treatment for a return packet flow that is associated with an originating packet flow in a network, comprising:
means for receiving the originating packet flow;
means for determining that one or more packets in the originating packet flow are marked with a first DSCP value that includes a request for application of the same quality of service treatment to the return packet flow;
means for creating and storing information identifying the originating packet flow and a second DSCP value for marking the return packet flow;
means for receiving the return packet flow and determining that it is associated with the originating packet flow;
means for marking packets of the return packet flow with the second DSCP value.

14. An apparatus as recited in Claim 13, wherein the information identifying the originating packet flow and the second DSCP value are created and stored in a flow table of a network switch that is acting as a policy enforcement point.

15. An apparatus as recited in Claim 13, wherein the information identifying the originating packet flow and the second DSCP value are created and stored in a network-based application recognition table of a network switch that is acting as a policy enforcement point.

16. An apparatus as recited in Claim 13, wherein the first DSCP value that includes a request for application of the same quality of service treatment to the return packet flow has a value that is one unit greater than the second DSCP value.

17. An apparatus as recited in Claim 13, wherein the steps are carried out at a switch device that is logically located at an edge point of a network.

18. An apparatus as recited in Claim 13, wherein the means for creating and storing information comprises a means for creating and storing a static policy at a policy server, wherein the static policy specifies applying the second DSCP value to the return packet flow.

19. An apparatus as recited in Claim 13, further comprising:
means for identifying an end of the originating packet flow;
means for removing the stored information that identifies the originating packet flow and a second DSCP value for marking the return packet flow.

20. An apparatus for automatically establishing differentiated services quality of service treatment for a return packet flow that is associated with an originating packet flow in a network, comprising:
a network interface that is coupled to the data network for receiving one or more packet flows therefrom;
~~a processor;~~

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

receiving the originating packet flow;

determining that one or more packets in the originating packet flow are marked with a DSCP value that matches a policy rule that requires setting a specified DSCP value in the return packet flow;

creating and storing information identifying the originating packet flow and a second DSCP value for marking the return packet flow;

receiving the return packet flow and determining that it is associated with the originating packet flow;

marking packets of the return packet flow with the second DSCP value.

20. An apparatus as recited in Claim 19, wherein the information identifying the originating packet flow and the second DSCP value are created and stored in a flow table of a network switch that is acting as a policy enforcement point.

21. An apparatus as recited in Claim 19, wherein the information identifying the originating packet flow and the second DSCP value are created and stored in a network-based application recognition table of a network switch that is acting as a policy enforcement point.

22. An apparatus as recited in Claim 19, wherein the steps are carried out at a switch device that is logically located at an edge point of a network.

23. An apparatus as recited in Claim 19, wherein creating and storing information comprises creating and storing a static policy at a policy server, wherein the static policy specifies applying the second DSCP value to the return packet flow.

24. An apparatus as recited in Claim 19, comprising further stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:
identifying an end of the originating packet flow;
removing the stored information that identifies the originating packet flow and a second DSCP value for marking the return packet flow.

25. A method of providing a selective automatic bi-directional differentiated services quality of service treatment guarantee for a return packet flow that is associated with an originating packet flow in a network, the method comprising the computer-implemented steps of:
creating and storing a first DSCP value and a second DSCP value that are both associated with the same per-hop-behavior (PHB) treatment at core network devices but are each associated with a different reflective DSCP setting;
receiving the originating packet flow;
receiving the return packet flow and determining that it is associated with the originating packet flow;
when one or more packets in the originating packet flow are marked with the first DSCP value, marking packets of the return packet flow with the second DSCP value;
when one or more packets in the originating packet flow are marked with the second DSCP value, passing packets of the return packet flow without modification of DSCP values in such packets.

26. A method as recited in Claim 25, wherein marking packets of the return packet flow is carried out only when the originating packet flow originates from a trusted interface.

27. A method as recited in Claim 1, wherein marking packets of the return packet flow is carried out only when the originating packet flow originates from a trusted interface.

28. A method as recited in Claim 1, wherein the steps of marking packets of the return packet flow with the second DSCP value comprises the steps of marking packets of the return packet flow with the second DSCP value only when the originating packet flow originates from a trusted interface.

add A2